

# [NT] Microsoft Commerce Server 2002 Authentication Bypass

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00051.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 19 Mar 2006 15:48:02 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Microsoft Commerce Server 2002 Authentication Bypass

---

## SUMMARY

" <<http://www.microsoft.com/commerceserver/default.msp>> Commerce Server 2002 is an extensible solution that enables organizations to rapidly deploy personalized portals. "

Improper authentication validation allows attackers to authenticate as an existing user in Microsoft Commerce Server 2002.

## DETAILS

Vulnerable Systems:

- \* Microsoft Commerce Server 2002

Immune Systems:

- \* Microsoft Commerce Server 2002 SP2

Microsoft Commerce Server is used by companies who want to give customers the opportunity to change their own details on the Internet or to buy products.

Companies who use it are: eCommerce sites or interactive companies.

## [NT] Microsoft Commerce Server 2002 Authentication Bypass

The problem is in the sample files of "authfiles". If you make your own Solution site in Commerce Server and the "authfiles" are installed on your server, you're vulnerable for positive user logon's using false passwords.

If you know a user (some sites uses an e-mail address) and you go to <http://site/authfiles/login.asp> (some sites have it in another directory) and you enter the Username and a false password you get an error.

After the error you go with the same browser to the root directory of the site <http://site/> You get another error and if you go again to the site you are logged on as the entered user.

Vendor Status:

The vendor has issued a warning :

<[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs\\_se\\_securityconcepts\\_cbgw.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securityconcepts_cbgw.asp)>  
[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs\\_se\\_securityconcepts\\_cbgw.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securityconcepts_cbgw.asp)

The vendor has issued a fix:

<<http://www.microsoft.com/downloads/details.aspx?familyid=58e6d658-cc3e-4846-8ef7-264e6eeb4c1e&displaylang=en>>  
<http://www.microsoft.com/downloads/details.aspx?familyid=58e6d658-cc3e-4846-8ef7-264e6eeb4c1e&displaylang=en>

Disclosure Timeline:

31-03-2003 – First contact  
26-08-2003 – Fixed in SP2  
17-03-2006 – Public Disclosure

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:d.vd.giessen@xxxxxxxxxx>>  
Dimitri.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.